Qualification Pack

Cloud Security Analyst

QP Code: SSC/Q8309

Version: 3.0

NSQF Level: 5

IT-ITeS Sector Skill Council || NASSCOM Plot No - 7, 8, 9 & 10, 3rd Floor, Sector 126 Noida Uttar Pradesh - 201303

Contents

Qualification Pack

SSC/Q8309: Cloud Security Analyst

Brief Job Description

Individuals in this role, monitor the cloud and IT assets associated with the organizations to check on security risks and threats. They manage and enforce security protocols and perform tests to identify potential security threats.

Personal Attributes

Cloud Security Analyst must be able to communicate effectively, build relationships with others and collaborate with various stakeholders. He/she must have a zeal to learn new things.

Applicable National Occupational Standards (NOS)

Compulsory NOS:

1. SSC/N8334: Detect, monitor and audit occurrences of information security threats and risks

2. SSC/N8335: Respond to security threats and restore affected capabilities

3. SSC/N8337: Monitor and maintain compliance of regulatory standards across the organization

4. SSC/N9014: Maintain an inclusive, environmentally sustainable workplace

5. DGT/VSQ/N0102: Employability Skills (60 Hours)

Qualification Pack (QP) Parameters

Sector	IT-ITeS
Sub-Sector	Future Skills
Occupation	Cloud Computing
Country	India
NSQF Level	5
Credits	16
Aligned to NCO/ISCO/ISIC Code	NCO-2015/2522.0201

Minimum Educational Qualification & Experience	Completed 2nd year of UG (UG Diploma) (UG Program of 3 or 4 years (Engineering/ Science)) OR Completed 2nd year diploma after 12th OR Previous relevant Qualification of NSQF Level (NSQF Level 4) with 3 Years of experience relevant experience in relevant field
Minimum Level of Education for Training in School	
Pre-Requisite License or Training	NA
Minimum Job Entry Age	20 Years
Last Reviewed On	NA
Next Review Date	28/07/2025
NSQC Approval Date	28/07/2022
Version	3.0
Reference code on NQR	QG-05-IT-00509-2023-V1.1-NASSCOM
NQR Version	3

SSC/N8334: Detect, monitor and audit occurrences of information security threats and risks

Description

This unit is about detecting threats and anomalies, employing continuous security monitoring processes, maintaining threat detection processes and performing audits.

Scope

The scope covers the following :

- Perform historical analysis of security threats/incidents
- Detect vulnerabilities & threats
- Monitor threats and security incidents
- Conduct security audits

Elements and Performance Criteria

Perform historical analysis of security threats/incidents

To be competent, the user/individual on the job must be able to:

PC1. gather information on previous security incidents and how were they managed by accessing the organization's knowledge base

Detect vulnerabilities & threats

To be competent, the user/individual on the job must be able to:

PC2. identify and implement automated security assessment tools to perform security assessments of cloud systems

PC3. perform vulnerability testing and risk analysis to identify security threats and vulnerabilities in the cloud solution in a timely manner

PC4. implement security controls to identify security anomalies in line with data security policies, procedures and guidelines

PC5. assess the potential impact of security anomalies on the organization

PC6. record, classify and prioritize security incidents using standard templates and tools

Monitor threats and security incidents

To be competent, the user/individual on the job must be able to:

PC7. perform regular review and maintenance of threat detection processes

PC8. report security threats and vulnerabilities to relevant stakeholders

PC9. develop KPIs for monitoring the security incidents and identifying the root cause

PC10. continuously monitor anomalies and incidents related to cloud security

PC11. leverage analytics to predict and extrapolate attack trends ahead of their occurrence

Conduct security audits

To be competent, the user/individual on the job must be able to:

PC12. identify requirements of audit for the cloud solution and assist in audit reviews, as required

PC13. liaise with appropriate people to gather data/information required for audits

PC14. carry out required audit tasks using standard tools and following established procedures/guidelines/checklists

PC15. report outcomes of the security audits to appropriate stakeholders

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. organizational policies, procedures and guidelines which relate to maintaining cloud solution security

KU2. organizational policies and procedures for sharing data

KU3. organizational policies for documenting and implementing security procedures

KU4. how to collaborate with stakeholders to define and execute security processes

KU5. the range of standard templates and tools available and how to use them

KU6. fundamentals of enterprise security

KU7. how to identify and resolve security vulnerabilities and incidents

KU8. common security issues and incidents that may require action and who to report them to

KU9. how to maintain records of monitoring activities

KU10. how to obtain and validate information related to security issues

KU11. how to prepare and submit security assessment reports and who to share these with

KU12. how to identify and refer anomalies in data

KU13. different types of threat assessment tests

KU14. different types of vulnerability assessment tests

KU15. different types of security standards and protocols

KU16. different types of compliance/regulatory standards

KU17. how to conduct security audits

KU18. how to define KPIs to monitor security threats

KU19. how to create security safeguards to prevent security threats

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. follow instructions, guidelines, procedures, rules and service level agreements

GS2. ask for clarification and advice from appropriate people

GS3. listen effectively and communicate accurate information

GS4. follow rule-based decision making processes

GS5. make decisions on suitable courses

GS6. plan and organize the work to achieve targets and deadlines

GS7. analyze data and activities

GS8. pass on relevant information to others

GS9. apply balanced judgments to different situations

GS10. check the work is complete and free from errors

GS11. contribute to the quality of team work

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
Perform historical analysis of security threats/incidents	**2**	**6**	**-**	**-**
PC1. gather information on previous security incidents and how were they managed by accessing the organization's knowledge base	2	6	-	-
Detect vulnerabilities & threats	**10**	**27**	**-**	**-**
PC2. identify and implement automated security assessment tools to perform security assessments of cloud systems	2	6	-	-
PC3. perform vulnerability testing and risk analysis to identify security threats and vulnerabilities in the cloud solution in a timely manner	2	6	-	-
PC4. implement security controls to identify security anomalies in line with data security policies, procedures and guidelines	1	4	-	-
PC5. assess the potential impact of security anomalies on the organization	2	6	-	-
PC6. record, classify and prioritize security incidents using standard templates and tools	3	5	-	-
Monitor threats and security incidents	**11**	**24**	**-**	**-**
PC7. perform regular review and maintenance of threat detection processes	3	5	-	-
PC8. report security threats and vulnerabilities to relevant stakeholders	1	4	-	-
PC9. develop KPIs for monitoring the security incidents and identifying the root cause	3	5	-	-
PC10. continuously monitor anomalies and incidents related to cloud security	3	5	-	-
PC11. leverage analytics to predict and extrapolate attack trends ahead of their occurrence	1	5	-	-
Conduct security audits	**4**	**16**	**-**	**-**

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC12. identify requirements of audit for the cloud solution and assist in audit reviews, as required	1	4	-	-
PC13. liaise with appropriate people to gather data/information required for audits	1	4	-	-
PC14. carry out required audit tasks using standard tools and following established procedures/guidelines/checklists	1	4	-	-
PC15. report outcomes of the security audits to appropriate stakeholders	1	4	-	-
NOS Total	**27**	**73**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N8334
NOS Name	Detect, monitor and audit occurrences of information security threats and risks
Sector	IT-ITeS
Sub-Sector	Future Skills
Occupation	Cloud Computing
NSQF Level	5
Credits	TBD
Version	2.0
Last Reviewed Date	NA
Next Review Date	03/05/2026
NSQC Clearance Date	03/05/2023

SSC/N8335: Respond to security threats and restore affected capabilities

Description

This unit is about responding to security incidents, preventing their expansion and ensuring timely restoration and recovery of affected capabilities.

Scope

The scope covers the following :

- Ensure adherence to security policies and standards
- Escalate and report security incidents
- Recover & restore affected systems

Elements and Performance Criteria

Ensure adherence to security policies and standards

To be competent, the user/individual on the job must be able to:

PC1. plan timely response and wherever applicable, automate responses to the detected security threats

PC2. execute post-incident processes and procedures in line with security policies, procedures and guidelines

PC3. maintain and update checklist, runbooks and playbooks on security incidents

Escalate and report security incidents

To be competent, the user/individual on the job must be able to:

PC4. assign information security incidents promptly to appropriate people for investigation/action

PC5. track progress of investigations of the information security incidents

PC6. escalate security incidents to appropriate people where progress does not comply with standards or service level agreements (SLAs)

PC7. liaise with stakeholders to gather, validate and provide information related to information security incidents, where required

PC8. report to management of any security breach to carry out further discussions with law enforcement agencies, if required

PC9. prepare and submit accurate reports on information security incidents using standard templates and tools

Recover & restore affected systems

To be competent, the user/individual on the job must be able to:

PC10. prevent further expansion of the security incident

PC11. carry out backups of security devices and applications in line with security policies, procedures and guidelines, when required

PC12. ensure timely restoration of cloud assets and systems affected by security incidents

PC13. update the organizations knowledge base promptly and accurately with information security incidents and how they were managed

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. organizational policies, procedures and guidelines which relate to maintaining cloud solution security

KU2. organizational policies and procedures for sharing data

KU3. organizational policies for documenting and implementing security procedures

KU4. how to collaborate with stakeholders to define and execute security processes

KU5. the range of standard templates and tools available and how to use them

KU6. fundamentals of enterprise security

KU7. different stages of incident management and his/her role in relation to these, including: identify, contain, cleanse, recover, close

KU8. how to restore and recover systems after a security incident

KU9. how to obtain and validate information related to security issues

KU10. how to prepare and submit security reports and who to share these with

KU11. how to identify and refer anomalies in data

KU12. different types of threat assessment tests

KU13. different types of vulnerability assessment tests

KU14. different types of security standards and protocols

KU15. different types of compliance/regulatory standards

KU16. how to maintain and update checklist, runbooks and playbooks on security incidents

KU17. how to create backup and secure data

KU18. different types of security monitoring tools

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. follow instructions, guidelines, procedures, rules and service level agreements

GS2. ask for clarification and advice from appropriate people

GS3. listen effectively and communicate accurate information

GS4. follow rule-based decision making processes

GS5. make decisions on suitable courses

GS6. plan and organize the work to achieve targets and deadlines

GS7. pass on relevant information to others

GS8. apply balanced judgments to different situations

GS9. apply good attention to detail

GS10. check the work is complete and free from errors

GS11. contribute to the quality of team work

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
Ensure adherence to security policies and standards	**8**	**16**	**-**	**-**
PC1. plan timely response and wherever applicable, automate responses to the detected security threats	3	6	-	-
PC2. execute post-incident processes and procedures in line with security policies, procedures and guidelines	2	4	-	-
PC3. maintain and update checklist, runbooks and playbooks on security incidents	3	6	-	-
Escalate and report security incidents	**14**	**27**	**-**	**-**
PC4. assign information security incidents promptly to appropriate people for investigation/action	2	4	-	-
PC5. track progress of investigations of the information security incidents	2	4	-	-
PC6. escalate security incidents to appropriate people where progress does not comply with standards or service level agreements (SLAs)	2	4	-	-
PC7. liaise with stakeholders to gather, validate and provide information related to information security incidents, where required	2	4	-	-
PC8. report to management of any security breach to carry out further discussions with law enforcement agencies, if required	3	6	-	-
PC9. prepare and submit accurate reports on information security incidents using standard templates and tools	3	5	-	-
Recover & restore affected systems	**9**	**26**	**-**	**-**
PC10. prevent further expansion of the security incident	2	7	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC11. carry out backups of security devices and applications in line with security policies, procedures and guidelines, when required	2	7	-	-
PC12. ensure timely restoration of cloud assets and systems affected by security incidents	3	5	-	-
PC13. update the organizations knowledge base promptly and accurately with information security incidents and how they were managed	2	7	-	-
NOS Total	**31**	**69**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N8335
NOS Name	Respond to security threats and restore affected capabilities
Sector	IT-ITeS
Sub-Sector	Future Skills
Occupation	Cloud Computing
NSQF Level	5
Credits	TBD
Version	2.0
Last Reviewed Date	NA
Next Review Date	03/05/2026
NSQC Clearance Date	03/05/2023

SSC/N8337: Monitor and maintain compliance of regulatory standards across the organization

Description

This unit is about ensuring compliance and implementation of regulatory standards across the organization.

Scope

The scope covers the following :

- Monitor regulatory compliance using tools
- Resolve issues related to non-compliance

Elements and Performance Criteria

Monitor regulatory compliance using tools

To be competent, the user/individual on the job must be able to:

PC1. identify and implement compatible tools and automated solutions for monitoring compliance of regulatory standards

PC2. monitor the configurations of the infrastructure to ensure that it adheres to security and regulatory/compliance best practices

PC3. ensure that existing compliance related processes and procedures are being followed, with enough documentary evidence

PC4. collect data about cloud services and continuously perform checks against predetermined security best practices and regulatory/ compliance guidelines

PC5. perform an analysis to determine level of risk exposure of the discovered misconfigurations

PC6. provide timely feedback related to information security on contracts and agreements to be issued or entered into by the organization

PC7. drive security initiatives in the organization to ensure compliance to security and regulatory standards

Resolve issues related to non-compliance

To be competent, the user/individual on the job must be able to:

PC8. undertake corrective actions or implement auto-remediation workflows and security controls to correct cases of noncompliance

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. organizational policies, procedures and guidelines which relate to maintaining solution security

KU2. organizational policies and procedures for sharing data

KU3. organizational policies for documenting and implementing security procedures

KU4. how to collaborate with stakeholders to define and execute security processes

KU5. the range of standard templates and tools available and how to use them

KU6. fundamentals of enterprise security

KU7. how to manage security configuration

KU8. different types of security standards to check for security threats

KU9. different types of regulatory/compliance standards

KU10. how to monitor implementation of regulatory/compliance standards

KU11. how to evaluate systems for wrong security configuration

KU12. how to automate the security monitoring processes

KU13. different types of tools for monitoring compliance/regulatory standards in the organization

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. ask for clarification and advice from appropriate people

GS2. listen effectively and communicate accurate information

GS3. work independently and collaboratively

GS4. communicate with others in writing

GS5. analyze the impact of architectural and design decisions on business and organization

GS6. pass on relevant information to others

GS7. check the work is complete and free from errors

GS8. work effectively in a customer facing environment

GS9. plan and organize the work to achieve targets and deadlines

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
Monitor regulatory compliance using tools	**27**	**63**	**-**	**-**
PC1. identify and implement compatible tools and automated solutions for monitoring compliance of regulatory standards	4	8	-	-
PC2. monitor the configurations of the infrastructure to ensure that it adheres to security and regulatory/compliance best practices	6	14	-	-
PC3. ensure that existing compliance related processes and procedures are being followed, with enough documentary evidence	6	14	-	-
PC4. collect data about cloud services and continuously perform checks against predetermined security best practices and regulatory/ compliance guidelines	6	14	-	-
PC5. perform an analysis to determine level of risk exposure of the discovered misconfigurations	3	7	-	-
PC6. provide timely feedback related to information security on contracts and agreements to be issued or entered into by the organization	1	3	-	-
PC7. drive security initiatives in the organization to ensure compliance to security and regulatory standards	1	3	-	-
Resolve issues related to non-compliance	**3**	**7**	**-**	**-**
PC8. undertake corrective actions or implement auto-remediation workflows and security controls to correct cases of noncompliance	3	7	-	-
NOS Total	**30**	**70**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N8337
NOS Name	Monitor and maintain compliance of regulatory standards across the organization
Sector	IT-ITeS
Sub-Sector	Future Skills
Occupation	Cloud Computing
NSQF Level	5
Credits	TBD
Version	2.0
Last Reviewed Date	NA
Next Review Date	03/05/2026
NSQC Clearance Date	03/05/2023

SSC/N9014: Maintain an inclusive, environmentally sustainable workplace

Description

The unit is about implementing and improving diversity equality and inclusion in a sustainable and environment friendly workplace.

Scope

The scope covers the following :

- Sustainable Practices
- Respect diversity and strengthen practices to promote equity (equality)/inclusivity

Elements and Performance Criteria

Sustainable Practices

To be competent, the user/individual on the job must be able to:

PC1. optimize usage of electricity/energy, materials, and water in various asks / activities / processes and plan the implementation of energy efficient systems in a phased manner

PC2. segregate recyclable, non-recyclable and hazardous waste generated for disposal or efficient waste management

Respect diversity and strengthen practices to promote equity (equality)/inclusivity

To be competent, the user/individual on the job must be able to:

PC3. understand the diversity policy of the organization and use internal & external communication to colleagues to improve

PC4. comply with PwD inclusive policies for an adaptable and equitable work environment

PC5. improve through specifically designed recruitment practices, PwD friendly infrastructure, job roles, etc.

PC6. use and advocate for appropriate verbal/nonverbal communication, schemes and benefits of PwD.

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. the organization's policies and procedures about gender inclusivity, equality and sustainability while working with colleagues and your role and responsibilities in relation to this

KU2. inclusive tools and practices of communication to acknowledge/validate, share and promote the cause of gender parity at workplace. For example - supporting women with mentorship programs, speaking out against discriminatory practices or harassment

KU3. the concept of gender, gender equality and gender discrimination, and all forms of gender discrimination, violence and inequality, including the current and historical causes of gender inequality in the workplace

KU4. how to maintain and provide a conducive work environment that is free from any harassment. facilities and amenities to PwD to perform and excel in their role

KU5. organization's redressal mechanisms (like the POSH committee) to address harassment and bias at the workplace, with awareness of prevalent legislations against bias and sexual harassment

KU6. initiatives towards efficient use of natural resources and energy, reduction and prevention of pollution and promoting waste avoidance and recycling measures in line with internationally disseminated technologies and practices

KU7. all about various energy options including renewable and non-renewable with their environmental impacts, health issues, usage, safety and energy security

KU8. implications that any non-compliance with electricity and energy may have on individuals and the organization

KU9. the organization's electricity first aid emergency procedures

KU10. how to monitor, measure and report performance of environmental conservation

KU11. different types of electricity accidents, safety and security and how and when to report these

KU12. how to use the electricity/energy safety, accident reporting, emergency procedures and the importance of these

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. read PwD instructions, guidelines, procedures, diversity policies/acts, rules and service level agreements

GS2. be aware of one's own gender identity and gender role.and respectful of the gender performances of others

GS3. organize team building or sensitization workshops to address gender biases, stereotypes and potentially blind spots

GS4. clarify personal norms and values related to energy production and usage as well as to reflect and evaluate their own energy usage in terms of efficiency and sufficiency

GS5. listen and communicate (oral) effectively and accurately on all PwD policies

GS6. apply balanced judgments in gender diversity situations

GS7. take action to reduce the carbon footprint of business activities and embed environmental responsibility

GS8. calibration session with employees to discuss gender biases, stereotypes and potentially blind spots

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
Sustainable Practices	**10**	**30**	**-**	**-**
PC1. optimize usage of electricity/energy, materials, and water in various asks / activities / processes and plan the implementation of energy efficient systems in a phased manner	5	15	-	-
PC2. segregate recyclable, non-recyclable and hazardous waste generated for disposal or efficient waste management	5	15	-	-
Respect diversity and strengthen practices to promote equity (equality)/inclusivity	**10**	**50**	**-**	**-**
PC3. understand the diversity policy of the organization and use internal & external communication to colleagues to improve	5	10	-	-
PC4. comply with PwD inclusive policies for an adaptable and equitable work environment	-	10	-	-
PC5. improve through specifically designed recruitment practices, PwD friendly infrastructure, job roles, etc.	-	20	-	-
PC6. use and advocate for appropriate verbal/nonverbal communication, schemes and benefits of PwD.	5	10	-	-
NOS Total	**20**	**80**	**-**	**-**

Qualification Pack

National Occupational Standards (NOS) Parameters

NOS Code	SSC/N9014
NOS Name	Maintain an inclusive, environmentally sustainable workplace
Sector	IT-ITeS
Sub-Sector	IT Services, Business Process Management, Engineering R&D, Software Product Development, Future Skills
Occupation	Generic,
NSQF Level	5
Credits	1
Version	1.0
Last Reviewed Date	27/01/2022
Next Review Date	28/04/2025
NSQC Clearance Date	28/04/2022

DGT/VSQ/N0102: Employability Skills (60 Hours)

Description

This unit is about employability skills, Constitutional values, becoming a professional in the 21st Century, digital, financial, and legal literacy, diversity and Inclusion, English and communication skills, customer service, entrepreneurship, and apprenticeship, getting ready for jobs and career development.

Scope

The scope covers the following :

- Introduction to Employability Skills
- Constitutional values - Citizenship
- Becoming a Professional in the 21st Century
- Basic English Skills
- Career Development & Goal Setting
- Communication Skills
- Diversity & Inclusion
- Financial and Legal Literacy
- Essential Digital Skills
- Entrepreneurship
- Customer Service
- Getting ready for Apprenticeship & Jobs

Elements and Performance Criteria

Introduction to Employability Skills

To be competent, the user/individual on the job must be able to:

PC1. identify employability skills required for jobs in various industries

PC2. identify and explore learning and employability portals

Constitutional values – Citizenship

To be competent, the user/individual on the job must be able to:

PC3. recognize the significance of constitutional values, including civic rights and duties, citizenship, responsibility towards society etc. and personal values and ethics such as honesty, integrity, caring and respecting others, etc.

PC4. follow environmentally sustainable practices

Becoming a Professional in the 21st Century

To be competent, the user/individual on the job must be able to:

PC5. recognize the significance of 21st Century Skills for employment

PC6. practice the 21st Century Skills such as Self-Awareness, Behaviour Skills, time management, critical and adaptive thinking, problem-solving, creative thinking, social and cultural awareness, emotional awareness, learning to learn for continuous learning etc. in personal and professional life

Basic English Skills

To be competent, the user/individual on the job must be able to:

PC7. use basic English for everyday conversation in different contexts, in person and over the telephone

PC8. read and understand routine information, notes, instructions, mails, letters etc. written in English

PC9. write short messages, notes, letters, e-mails etc. in English

Career Development & Goal Setting

To be competent, the user/individual on the job must be able to:

PC10. understand the difference between job and career

PC11. prepare a career development plan with short- and long-term goals, based on aptitude

Communication Skills

To be competent, the user/individual on the job must be able to:

PC12. follow verbal and non-verbal communication etiquette and active listening techniques in various settings

PC13. work collaboratively with others in a team

Diversity & Inclusion

To be competent, the user/individual on the job must be able to:

PC14. communicate and behave appropriately with all genders and PwD

PC15. escalate any issues related to sexual harassment at workplace according to POSH Act

Financial and Legal Literacy

To be competent, the user/individual on the job must be able to:

PC16. select financial institutions, products and services as per requirement

PC17. carry out offline and online financial transactions, safely and securely

PC18. identify common components of salary and compute income, expenses, taxes, investments etc

PC19. identify relevant rights and laws and use legal aids to fight against legal exploitation

Essential Digital Skills

To be competent, the user/individual on the job must be able to:

PC20. operate digital devices and carry out basic internet operations securely and safely

PC21. use e- mail and social media platforms and virtual collaboration tools to work effectively

PC22. use basic features of word processor, spreadsheets, and presentations

Entrepreneurship

To be competent, the user/individual on the job must be able to:

PC23. identify different types of Entrepreneurship and Enterprises and assess opportunities for potential business through research

PC24. develop a business plan and a work model, considering the 4Ps of Marketing Product, Price, Place and Promotion

PC25. identify sources of funding, anticipate, and mitigate any financial/ legal hurdles for the potential business opportunity

Customer Service

To be competent, the user/individual on the job must be able to:

PC26. identify different types of customers

PC27. identify and respond to customer requests and needs in a professional manner.

PC28. follow appropriate hygiene and grooming standards

Getting ready for apprenticeship & Jobs

To be competent, the user/individual on the job must be able to:

PC29. create a professional Curriculum vitae (Résumé)

PC30. search for suitable jobs using reliable offline and online sources such as Employment exchange, recruitment agencies, newspapers etc. and job portals, respectively

PC31. apply to identified job openings using offline /online methods as per requirement

PC32. answer questions politely, with clarity and confidence, during recruitment and selection

PC33. identify apprenticeship opportunities and register for it as per guidelines and requirements

Knowledge and Understanding (KU)

The individual on the job needs to know and understand:

KU1. need for employability skills and different learning and employability related portals

KU2. various constitutional and personal values

KU3. different environmentally sustainable practices and their importance

KU4. Twenty first (21st) century skills and their importance

KU5. how to use English language for effective verbal (face to face and telephonic) and written communication in formal and informal set up

KU6. importance of career development and setting long- and short-term goals

KU7. about effective communication

KU8. POSH Act

KU9. Gender sensitivity and inclusivity

KU10. different types of financial institutes, products, and services

KU11. how to compute income and expenditure

KU12. importance of maintaining safety and security in offline and online financial transactions

KU13. different legal rights and laws

KU14. different types of digital devices and the procedure to operate them safely and securely

KU15. how to create and operate an e- mail account and use applications such as word processors, spreadsheets etc.

KU16. how to identify business opportunities

KU17. types and needs of customers

KU18. how to apply for a job and prepare for an interview

KU19. apprenticeship scheme and the process of registering on apprenticeship portal

Generic Skills (GS)

User/individual on the job needs to know how to:

GS1. read and write different types of documents/instructions/correspondence

GS2. communicate effectively using appropriate language in formal and informal settings

GS3. behave politely and appropriately with all

GS4. how to work in a virtual mode

GS5. perform calculations efficiently

GS6. solve problems effectively

GS7. pay attention to details

GS8. manage time efficiently

GS9. maintain hygiene and sanitization to avoid infection

Assessment Criteria

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
Introduction to Employability Skills	1	1	-	-
PC1. identify employability skills required for jobs in various industries	-	-	-	-
PC2. identify and explore learning and employability portals	-	-	-	-
Constitutional values – Citizenship	1	1	-	-
PC3. recognize the significance of constitutional values, including civic rights and duties, citizenship, responsibility towards society etc. and personal values and ethics such as honesty, integrity, caring and respecting others, etc.	-	-	-	-
PC4. follow environmentally sustainable practices	-	-	-	-
Becoming a Professional in the 21st Century	2	4	-	-
PC5. recognize the significance of 21st Century Skills for employment	-	-	-	-
PC6. practice the 21st Century Skills such as Self-Awareness, Behaviour Skills, time management, critical and adaptive thinking, problem-solving, creative thinking, social and cultural awareness, emotional awareness, learning to learn for continuous learning etc. in personal and professional life	-	-	-	-
Basic English Skills	2	3	-	-
PC7. use basic English for everyday conversation in different contexts, in person and over the telephone	-	-	-	-
PC8. read and understand routine information, notes, instructions, mails, letters etc. written in English	-	-	-	-
PC9. write short messages, notes, letters, e-mails etc. in English	-	-	-	-
Career Development & Goal Setting	1	2	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
PC10. understand the difference between job and career	-	-	-	-
PC11. prepare a career development plan with short- and long-term goals, based on aptitude	-	-	-	-
Communication Skills	**2**	**2**	**-**	**-**
PC12. follow verbal and non-verbal communication etiquette and active listening techniques in various settings	-	-	-	-
PC13. work collaboratively with others in a team	-	-	-	-
Diversity & Inclusion	**1**	**2**	**-**	**-**
PC14. communicate and behave appropriately with all genders and PwD	-	-	-	-
PC15. escalate any issues related to sexual harassment at workplace according to POSH Act	-	-	-	-
Financial and Legal Literacy	**2**	**3**	**-**	**-**
PC16. select financial institutions, products and services as per requirement	-	-	-	-
PC17. carry out offline and online financial transactions, safely and securely	-	-	-	-
PC18. identify common components of salary and compute income, expenses, taxes, investments etc	-	-	-	-
PC19. identify relevant rights and laws and use legal aids to fight against legal exploitation	-	-	-	-
Essential Digital Skills	**3**	**4**	**-**	**-**
PC20. operate digital devices and carry out basic internet operations securely and safely	-	-	-	-
PC21. use e- mail and social media platforms and virtual collaboration tools to work effectively	-	-	-	-
PC22. use basic features of word processor, spreadsheets, and presentations	-	-	-	-

Assessment Criteria for Outcomes	Theory Marks	Practical Marks	Project Marks	Viva Marks
Entrepreneurship	**2**	**3**	**-**	**-**
PC23. identify different types of Entrepreneurship and Enterprises and assess opportunities for potential business through research	-	-	-	-
PC24. develop a business plan and a work model, considering the 4Ps of Marketing Product, Price, Place and Promotion	-	-	-	-
PC25. identify sources of funding, anticipate, and mitigate any financial/ legal hurdles for the potential business opportunity	-	-	-	-
Customer Service	**1**	**2**	**-**	**-**
PC26. identify different types of customers	-	-	-	-
PC27. identify and respond to customer requests and needs in a professional manner.	-	-	-	-
PC28. follow appropriate hygiene and grooming standards	-	-	-	-
Getting ready for apprenticeship & Jobs	**2**	**3**	**-**	**-**
PC29. create a professional Curriculum vitae (Résumé)	-	-	-	-
PC30. search for suitable jobs using reliable offline and online sources such as Employment exchange, recruitment agencies, newspapers etc. and job portals, respectively	-	-	-	-
PC31. apply to identified job openings using offline /online methods as per requirement	-	-	-	-
PC32. answer questions politely, with clarity and confidence, during recruitment and selection	-	-	-	-
PC33. identify apprenticeship opportunities and register for it as per guidelines and requirements	-	-	-	-
NOS Total	**20**	**30**	**-**	**-**

National Occupational Standards (NOS) Parameters

NOS Code	DGT/VSQ/N0102
NOS Name	Employability Skills (60 Hours)
Sector	Cross Sectoral
Sub-Sector	Professional Skills
Occupation	Employability
NSQF Level	4
Credits	2
Version	1.0
Last Reviewed Date	23/06/2023
Next Review Date	23/06/2026
NSQC Clearance Date	23/06/2023

Assessment Guidelines and Assessment Weightage

Assessment Guidelines

1. Criteria for assessment for each Qualification Pack will be created by the Sector Skill Council. Each Performance Criteria (PC) will be assigned marks proportional to its importance in NOS. SSC will also lay down the proportion of marks for Theory and Skills Practical for each PC.

2. The assessment for the theory part will be based on the knowledge bank of questions created by the SSC.

3. Assessment will be conducted for all compulsory NOS, and where applicable, on the selected elective/option NOS/set of NOS.

4. Individual assessment agencies will create unique question papers for the theory part for each candidate at each examination/training center (as per the assessment criteria below).

5. Individual assessment agencies will create unique evaluations for skill practical for every student at each examination/training center based on this criterion.

6. To pass a QP, a trainee should score an average of 70% or more.

7. In case of unsuccessful completion, the trainee may seek reassessment on the Qualification Pack.

Minimum Aggregate Passing % at QP Level : 70

(**Please note**: Every Trainee should score a minimum aggregate passing percentage as specified above, to successfully clear the Qualification Pack assessment.)

Assessment Weightage

Compulsory NOS

National Occupational Standards	Theory Marks	Practical Marks	Project Marks	Viva Marks	Total Marks	Weightage
SSC/N8334.Detect, monitor and audit occurrences of information security threats and risks	27	73	-	-	100	25
SSC/N8335.Respond to security threats and restore affected capabilities	31	69	-	-	100	25
SSC/N8337.Monitor and maintain compliance of regulatory standards across the organization	30	70	-	-	100	25
SSC/N9014.Maintain an inclusive, environmentally sustainable workplace	20	80	-	-	100	10
DGT/VSQ/N0102.Employability Skills (60 Hours)	20	30	0	0	50	15
Total	**128**	**322**	**-**	**-**	**450**	**100**

Acronyms

NOS	National Occupational Standard(s)
NSQF	National Skills Qualifications Framework
QP	Qualifications Pack
TVET	Technical and Vocational Education and Training
SPD	Software Product Development
ERD	Engineering and R&D
ITS	Information Technology Services
BPM	Business Process Management
IT-ITeS	Information Technology - Information Technology enabled Services
BPM	Business Process Management
BPO	Business Process Outsourcing
KPO	Knowledge Process Outsourcing
LPO	LPO
IPO	Information Process Outsourcing
IT-ITeS	Information Technology - Information Technology enabled Services
BPM	Business Process Management
BPO	Business Process Outsourcing
KPO	Knowledge Process Outsourcing
LPO	LPO
IPO	Information Process Outsourcing

Glossary

Sector	Sector is a conglomeration of different business operations having similar business and interests. It may also be defined as a distinct subset of the economy whose components share similar characteristics and interests.
Sub-sector	Sub-sector is derived from a further breakdown based on the characteristics and interests of its components.
Occupation	Occupation is a set of job roles, which perform similar/ related set of functions in an industry.
Job role	Job role defines a unique set of functions that together form a unique employment opportunity in an organisation.
Occupational Standards (OS)	OS specify the standards of performance an individual must achieve when carrying out a function in the workplace, together with the Knowledge and Understanding (KU) they need to meet that standard consistently. Occupational Standards are applicable both in the Indian and global contexts.
Performance Criteria (PC)	Performance Criteria (PC) are statements that together specify the standard of performance required when carrying out a task.
National Occupational Standards (NOS)	NOS are occupational standards which apply uniquely in the Indian context.
Qualifications Pack (QP)	QP comprises the set of OS, together with the educational, training and other criteria required to perform a job role. A QP is assigned a unique qualifications pack code.
Unit Code	Unit code is a unique identifier for an Occupational Standard, which is denoted by an 'N'
Unit Title	Unit title gives a clear overall statement about what the incumbent should be able to do.
Description	Description gives a short summary of the unit content. This would be helpful to anyone searching on a database to verify that this is the appropriate OS they are looking for.
Scope	Scope is a set of statements specifying the range of variables that an individual may have to deal with in carrying out the function which have a critical impact on quality of performance required.

Knowledge and Understanding (KU)	Knowledge and Understanding (KU) are statements which together specify the technical, generic, professional and organisational specific knowledge that an individual needs in order to perform to the required standard.
Organisational Context	Organisational context includes the way the organisation is structured and how it operates, including the extent of operative knowledge managers have of their relevant areas of responsibility.
Technical Knowledge	Technical knowledge is the specific knowledge needed to accomplish specific designated responsibilities.
Core Skills/ Generic Skills (GS)	Core skills or Generic Skills (GS) are a group of skills that are the key to learning and working in today's world. These skills are typically needed in any work environment in today's world. These skills are typically needed in any work environment. In the context of the OS, these include communication related skills that are applicable to most job roles.
Electives	Electives are NOS/set of NOS that are identified by the sector as contributive to specialization in a job role. There may be multiple electives within a QP for each specialized job role. Trainees must select at least one elective for the successful completion of a QP with Electives.
Options	Options are NOS/set of NOS that are identified by the sector as additional skills. There may be multiple options within a QP. It is not mandatory to select any of the options to complete a QP with Options.
Helpdesk	Helpdesk is an entity to which the customers will report their IT problems. IT Service Helpdesk Attendant is responsible for managing the helpdesk.
Helpdesk	Helpdesk is an entity to which the customers will report their IT problems. IT Service Helpdesk Attendant is responsible for managing the helpdesk.